

Hacker Report Details by Dialed Number

Xiox Corporation
577 Airport Blvd
Burlingame, CA 94030
(415) 375-8188

CALL DATES: 1/1/92 through 12/31/92

DATA FILE NAME: C:CALldata.DAT

SORTED BY: Extension, Dialed Number

PAGE 1

DATE PRINTED: 04-01-1992 at 18:22:34

EXTENSION	DATE	TIME	DAC	DIALED NUMBER CITY/STATE	MIN	COST
3	4/02/92	2:56p	91	(414) 456-7890	20.6	\$5.25
3	4/02/92	2:56p	91	(414) 456-7890	20.6	\$5.25
3	4/01/92	8:45	91	(809) 456-7890 Saint Vincent, SV	15.3	\$3.98

EXTENSION	USER NAME	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
3		3	\$14.48	56.5	18.8	\$4.83	\$0.26

4	4/01/92	10:56	91	(809) 456-7890 Saint Vincent, SV	16.3	\$4.23
---	---------	-------	----	----------------------------------	------	--------

EXTENSION	USER NAME	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
4		1	\$4.23	16.3	16.3	\$4.23	\$0.26

REPORT TOTAL

COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
4	\$18.71	72.8	18.2	\$4.68	\$0.26

International Calls

Xiox Corporation
577 Airport Blvd
Burlingame, CA 94030
(415) 375-8188

CALL DATES: 1/1/92 through 1/31/92
DATA FILE NAME: C:CALldata.DAT
SORTED BY: Dialed Number, Extension

PAGE 1
DATE PRINTED: 04-01-1992 at 18:18:33

EXTENSION	DATE	TIME	DAC	DIALED NUMBER	CITY/STATE	MIN	COST
254	1/21/92	7:22	9011	447 16291041	Unit.Kingdom	2.7	\$2.79
254	1/22/92	6:57	9011	447 16291041	Unit.Kingdom	1.5	\$1.34
254	1/23/92	7:01	9011	447 16291041	Unit.Kingdom	7.0	\$6.49
224	1/31/92	8:20	9011	492 08426837	Fed.Rep.Ger.	0.8	\$1.47
224	1/31/92	8:20	9011	499 11685577	Fed.Rep.Ger.	2.7	\$3.41
241	1/20/92	8:29	9011	507 52442	Panama	1.0	\$1.71
241	1/20/92	8:31	9011	507 52442	Panama	1.5	\$2.08
224	1/23/92	4:43p	9011	612 5333277	Australia	7.7	\$10.56
222	1/27/92	9:43	9011	639 125030244	Philippines	0.9	\$2.50

REPORT TOTAL

COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
9	\$32.35	25.8	2.9	\$3.59	\$1.25

EXTENSION SUMMARY

FOR ALL CALLS

Xiox Corporation
 577 Airport Blvd
 Burlingame, CA 94030
 (415) 375-8188

CALL DATES: 1/1/92 through 12/31/92

DATA FILE NAME: C:CALldata.DAT

SORTED BY: Extension

PAGE 1

DATE PRINTED: 04-01-1992 at 18:26:42

EXTENSION	USER NAME	COUNT	MIN	COST	MIN/ CALL	COST/ CALL	COST/ MIN
1	FRONT DESK	1617	3340.1	\$83.07	2.1	\$0.05	\$0.02
3		3	56.5	\$14.48	18.8	\$4.83	\$0.26
4		1	16.3	\$4.23	16.3	\$4.23	\$0.26
200	CREED ERIKSON	20	51.1	\$8.41	2.6	\$0.42	\$0.16
201	TINA WISE	273	984.5	\$52.26	3.6	\$0.19	\$0.05
202	COPY ROOM	26	60.0	\$5.35	2.3	\$0.21	\$0.09
203	KITCHEN	10	8.8	\$0.32	0.9	\$0.03	\$0.04
204	RECEPTION AREA	32	101.0	\$1.11	3.2	\$0.03	\$0.01
210	CHIP FILAK	212	729.7	\$31.15	3.4	\$0.15	\$0.04
211	RITA PATEL	232	664.4	\$67.23	2.9	\$0.29	\$0.10
212	STUART MEYER	302	1080.9	\$69.29	3.6	\$0.23	\$0.06
220	RAMONA RUSSELL	37	78.7	\$6.13	2.1	\$0.17	\$0.08
221	PAT FUETSCH	235	520.5	\$68.15	2.2	\$0.29	\$0.13
222	GREG DAVIDSON	705	3236.9	\$558.25	4.6	\$0.79	\$0.17
223	BEN SLICK	516	2828.9	\$299.53	5.5	\$0.58	\$0.11
224	RICHARD FRICKE	361	1778.9	\$371.56	4.9	\$1.03	\$0.21
225	BOB BOYD	599	2592.6	\$255.15	4.3	\$0.43	\$0.10
226	PHIL MIKKELSON	236	816.3	\$203.03	3.5	\$0.86	\$0.25
227	RICK WINGET	348	987.3	\$91.89	2.8	\$0.26	\$0.09
228	MIKE O'CONNELL	429	3209.1	\$381.88	7.5	\$0.89	\$0.12
229	BOARD ROOM	196	815.5	\$89.54	4.2	\$0.46	\$0.11
240	BILL WELLING	138	731.1	\$93.73	5.3	\$0.68	\$0.13
241	JIM CRITCHFIELD	529	2638.2	\$244.57	5.0	\$0.46	\$0.09
242	REINE THIBEAULT	370	1842.9	\$217.18	5.0	\$0.59	\$0.12
243	C. ALTOMARE	496	1906.6	\$262.99	3.8	\$0.53	\$0.14
244	DONNA JONES	659	3082.9	\$389.25	4.7	\$0.59	\$0.13
251	VACANT	146	625.3	\$92.61	4.3	\$0.63	\$0.15
252	BLAINE DEAL	20	34.8	\$1.31	1.7	\$0.07	\$0.04
253	SARAH GERKEN	48	261.5	\$4.86	5.4	\$0.10	\$0.02
254	DAVE SCHLOSSMAN	288	1964.1	\$165.85	6.8	\$0.58	\$0.08
260	DIANE SCHWARTZ	819	3424.5	\$463.70	4.2	\$0.57	\$0.14
261	TRAINING	10	27.7	\$4.74	2.8	\$0.47	\$0.17
270	DIANA BRETZ	83	385.6	\$25.01	4.6	\$0.30	\$0.06
271	DENNIS BRETZ	51	154.5	\$8.85	3.0	\$0.17	\$0.06
272	ANI ARMSTRONG	107	297.6	\$11.72	2.8	\$0.11	\$0.04
273	Next to Tina's	7	30.4	\$1.19	4.3	\$0.17	\$0.04
274	Next to Sarah's	8	142.4	\$30.30	17.8	\$3.79	\$0.21

FOR ALL CALLS

PAGE 2

DATE PRINTED: 04-01-1992 at 18:26:42

EXTENSION	USER NAME	COUNT	MIN	COST	MIN/ CALL	COST/ CALL	COST/ MIN
275	Outside Ben's	1	0.4	\$0.00	0.4	\$0.00	\$0.00
280	SHEREE BAYLO	317	728.0	\$69.68	2.3	\$0.22	\$0.10
290	Carl Steffens	36	93.6	\$11.20	2.6	\$0.31	\$0.12
299	PRODUCT SUPPORT	223	293.5	\$0.00	1.3	\$0.00	\$0.00
373		4	7.8	\$0.70	2.0	\$0.18	\$0.09
390		21	88.7	\$8.41	4.2	\$0.40	\$0.09
392	VOICE MAIL	2500	4864.7	\$7.71	1.9	\$0.00	\$0.00
399		35	39.1	\$10.84	1.1	\$0.31	\$0.28

|REPORT TOTAL

COUNT	MIN	COST	MIN/ CALL	COST/ CALL	COST/ MIN
13306	47623.9	\$4788.41	3.6	\$0.36	\$0.10

809 Calls

Xiox Corporation
577 Airport Blvd
Burlingame, CA 94030
(415) 375-8188

CALL DATES: 1/1/92 through 1/31/92
DATA FILE NAME: C:CALldata.DAT
SORTED BY: Dialed Number, Extension

PAGE 1
DATE PRINTED: 04-01-1992 at 18:18:04

EXTENSION	DATE	TIME	DAC	DIALED NUMBER CITY/STATE	MIN	COST
244	1/14/92	8:59	9	(809) 258-9375 Caguas, PR	0.2	\$0.30
244	1/16/92	10:01	9	(809) 258-9375 Caguas, PR	0.3	\$0.30
244	1/16/92	10:44	9	(809) 258-9375 Caguas, PR	0.3	\$0.30
244	1/16/92	5:12p	9	(809) 258-9375 Caguas, PR	0.3	\$0.20
244	1/21/92	10:11	9	(809) 258-9375 Caguas, PR	0.2	\$0.30
244	1/27/92	8:54	9	(809) 258-9375 Caguas, PR	0.3	\$0.30
244	1/27/92	8:59	9	(809) 258-9375 Caguas, PR	0.4	\$0.30
244	1/29/92	1:04p	9	(809) 258-9375 Caguas, PR	0.3	\$0.30

DIALED NUMBER	CITY/STATE	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
(809) 258-9375	Caguas, PR	8	\$2.30	2.3	0.3	\$0.29	\$1.00

221	1/07/92	3:55p	91	(809) 787-4001 Bayamon, PR	0.7	\$0.30
221	1/09/92	10:26	91	(809) 787-4001 Bayamon, PR	2.6	\$0.88
221	1/24/92	11:55	91	(809) 787-4001 Bayamon, PR	2.6	\$0.88

DIALED NUMBER	CITY/STATE	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
(809) 787-4001	Bayamon, PR	3	\$2.06	5.9	2.0	\$0.69	\$0.35

260	1/10/92	11:03	91	(809) 926-9632 Jamaica, JM	29.3	\$22.84
260	1/15/92	11:36	91	(809) 926-9632 Jamaica, JM	4.0	\$3.34
260	1/24/92	1:46p	91	(809) 926-9632 Jamaica, JM	3.6	\$3.34
260	1/27/92	8:29	91	(809) 926-9632 Jamaica, JM	0.3	\$1.09
260	1/27/92	8:30	91	(809) 926-9632 Jamaica, JM	28.5	\$22.09
260	1/27/92	8:58	91	(809) 926-9632 Jamaica, JM	0.3	\$1.09
260	1/27/92	8:59	91	(809) 926-9632 Jamaica, JM	0.3	\$1.09
260	1/27/92	8:59	91	(809) 926-9632 Jamaica, JM	5.7	\$4.84
260	1/27/92	9:05	91	(809) 926-9632 Jamaica, JM	0.3	\$1.09
260	1/27/92	9:07	91	(809) 926-9632 Jamaica, JM	3.0	\$2.59
260	1/27/92	10:03	91	(809) 926-9632 Jamaica, JM	1.2	\$1.84
260	1/27/92	11:38	91	(809) 926-9632 Jamaica, JM	2.9	\$2.59
260	1/29/92	12:44p	91	(809) 926-9632 Jamaica, JM	4.9	\$4.09
260	1/31/92	8:13	91	(809) 926-9632 Jamaica, JM	1.8	\$1.84

809 Calls

PAGE 2

DATE PRINTED: 04-01-1992 at 18:18:04

DIALED NUMBER	CITY/STATE	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
(809) 926-9632	Jamaica, JM	14	\$73.76	86.1	6.2	\$5.27	\$0.86

REPORT TOTAL						
	COUNT	COST	MIN	MIN/ CALL	COST/ CALL	COST/ MIN
	25	\$78.12	94.3	3.8	\$3.12	\$0.83

During the 1980s, American business became well aware of hackers on computer networks and the millions of dollars in damage and expense they cause. The '90s have ushered in a new corporate thief: the telephone hacker.

Until recently, telephone fraud was mostly limited to employees placing long or expensive personal calls during business hours. Telecom managers learned that they could significantly reduce telephone costs from employee abuse by using call accounting and reporting systems to uncover expensive personal calls. Those simple halcyon days are gone.

A rapidly mushrooming area of abuse today is coming from outside the organization. With the increased sophistication of PBXs, and the granting of external access to the PBX by legitimate users, telephone hackers have found a lucrative side niche breaking into organizations' phone systems and placing or selling long distance calls.

It often happens in the middle of the night or over the weekend. Phone hackers use computers with auto-dialing modems to break your security password and gain access to your telephone system. Once inside your PBX, they can use or resell your long distance services to third parties, leaving you holding the bill.

Hackers use various methods to enter your phone system. One method is through a Direct Inward System Access (DISA) feature on some PBXs. By using a computer to repeatedly dial your number and then attempt to break the password by feeding in possible codes, the hacker may be

able to gain entry.

Unfortunately, some telecom managers make this process ridiculously easy by failing to take advantage of even minimal security features already available on their PBX, like password protection. Some don't even bother to reset the default password.

A second method used to gain access is through remote diagnostic numbers used for system administration. The more technically sophisticated switches have features that allow a vendor or service personnel to dial-in to the PBX and remotely diagnose and fix problems. Unfortunately, this same capability can also allow hackers in.

The consequences of fraud can be alarming. A single company can incur unauthorized charges of hundreds of thousands of dollars per month. Throughout the US, the scope of the problem is enormous. It is estimated that the total losses range from \$500 million to \$5 billion annually. And carriers, to this point, have been insistent on payment for the fraudulent calls.

Warning signs

The first sign most companies see of a hacker's activity is an increase in their long distance bill. Usually, the increase in call volume is sudden, not gradual. Unfortunately, the bill which includes the unauthorized charges may arrive up to four weeks after the beginning of the abuse, enough time to add up to a phenomenal expense.

With a call accounting system, the abuse

will show up much sooner. By running a weekly audit report, unusually high long distance charges will be much more readily apparent. Call accounting systems which can analyze and sort your call records in an almost unlimited fashion and allow you to create customized reports can give you the knowledge and flexibility to stay ahead of a hacker. In addition, weekly summary reports of trunk and extension traffic will highlight any fictitious or phantom extensions, which may also indicate illegal access, and which in any case you're being billed for.

Once a problem is suspected, detail reports on the particular trunk and extension will reveal the type of calls and extent of the problem. The flexibility of the call accounting system chosen will determine how effective the telecom manager is in trapping the hacker.

The type of PBX can also assist in fraud prevention. PBX switches like the AT&T Definity which create call records on all calls, including uncompleted attempts, allow the telecom manager to use call accounting software to report on repeated dial-in attempts, which often indicate an attempt to crack the access passwords. By seeing the clear trail of the hacker's tracks, a telecom manager can identify and close points of entry as quickly as a hacker finds them.

"We've been breached!"

One company which experienced and overcame telephone hackers is Advanced Micro Devices of Sunnyvale, CA. In April of 1990, Renee Seay, Manager of Telecommunications Applica-

HACKER TRACKS

by STUART D. MEYER

tions and Services at AMD, was notified by their long distance carrier, AT&T, that they may have a toll fraud problem. After examining their long distance bills, Renee noticed increased international traffic, greater than their calling activity warranted.

Determining how the hacker was obtaining access to their AT&T Definity PBX switch wasn't an obvious matter. Seay arranged to purchase a Xiox call accounting system to help identify the problem, as well as track and report on their normal telecommunications traffic.

With the proper means of analysis, Seay was quickly able to reveal the scope of the problem. By using Extension Summary and Trunk Reports, she was able to pinpoint exactly how, when, and where the fraudulent calls were being made.

The reports revealed thousands of dollars of calls per month being routed from Germany through AMD's remote access trunk. These calls were then placed from the PBX to locations all over the world. Somehow the hacker had gained access to the company's PBX and was re-selling long distance service to European callers, who were probably unaware of their participation in the illegal scheme.

The next step was to determine the hacker's methods of entry. Using the Xiox customer reporting capabilities to track their activity, Seay spent numerous hours monitoring their usage

and discovering their points of access. She placed additional security on dial access trunks to block calls being made from the PBX, and hoped this would provide the necessary barriers.

Unfortunately, the hacker was both persistent and experienced. Within a month, the weekly reports showed unusual trunk traffic and call records.

The hacker had found another way in! By printing the call detail reports on the trunk with unusual activity, Seay was able to see each of their attempts, both their methodology and pattern of hacking, and the point of successful entry. She was then able to immediately close the access and stop the unauthorized traffic.

The final solution involved removing AMD's German remote access trunk, which was the latest point of entry. Additionally, Seay replaced the existing line with a new line which requires two levels of security codes. Making these changes, she was able to shut down the illegal activity.

Now AMD is able to stay one step ahead of any illegal entry to their phone system. By monitoring the traffic on their trunks and extensions with the Model 6000 call accounting system, they are immediately alerted to any unusual increase in call volume or cost. If Seay does notice anything unusual, she can print detail reports, which show a clear trail of any attempted entry. AMD is

now in control of their PBX, and thus their telephone costs.

Conclusion

Hacking is not just the after-school activity of clever adolescents. It is also the occupation of skilled engineers and professionals. And it is not just an occasional call to Tibet, but an ongoing part of the daily business of a sophisticated international operation. Illegal telephone charges cost American companies millions of dollars per year.

All three major long distance carriers suggest fraud prevention programs to their customers, but say that companies are liable for all calls made through their PBXs, whether those calls are legitimate or fraudulent in nature. Thus, it is up to each telecom manager to protect their system from major intruders as well as minor abuses.

Fortunately, the tools exist to put the telecom manager on the same footing as the best hackers. Regular monitoring and the right equipment can shut down illegal and expensive telephone abuse—and put hackers where they belong: flat out of business. ■

Stuart D. Meyer is the Director of Product Marketing for Xiox Corp. in Burlingame, CA. He holds a BS in Economics from UC Berkeley.

Reprinted from Procomm Magazine, June, 1991. Copyright © 1991 Procomm Enterprises Magazine. All rights reserved. Call Procomm at (415) 459-4669 for more information.

XIOX CORPORATION

Inside Sales Representatives

Ben Slick - VP of Sales; Bob Boyd - Manager (415)375-8188

